ORIGINAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	
VS.	§	CRIMINAL NO. 3:08-CR-171-M
	§	(Supersedes Indictment returned on
MATTHEW DOUGLAS WEIGMAN (1)	§	June 3, 2008)

FACTUAL RESUME

Essential Elements:

1. In support of the plea of guilty to the two count superseding information charging in Count One a violation of 18 U.S.C. §1513(f), that being Conspiracy to Retaliate Against a Witness, Victim, or an Informant (U.S.C. §1513(e), and in Count Two charging a violation of 18 U.S.C. §371, that is Conspiracy to commit Access Device Fraud (18 U.S.C. §1029(a)(9)) and Unauthorized Access of Protected Computer (18 U.S.C. §1030(a)(5)(A)(ii) and (B)(iv)), the parties have stipulated and agreed to the essential elements of the offense and the facts.

2. The essential elements of Count One of the superseding information, Conspiracy to Retaliate Against a Witness, Victim, or an Informant (18 U.S.C. §1513(f)), are that

First: The defendant and at least one other person made an agreement to commit the crime, as charged in the indictment

Second: The defendant knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and

Third: The object of the conspiracy was to retaliate against a witness, victim, or an informant, in violation of 18 U.S.C. §1513(e).

3. The essential elements of the object of the conspiracy alleged in Count One of the superseding information, that is to Retaliate Against a Witness, Victim, or an Informant in violation of 18 U.S.C. §1513(e), are that

First: The defendant knowingly, with the intent to retaliate, took an action to interfere with the lawful employment or livelihood of WS,

Second: The defendant did so with intent to retaliate against WS because WS had provided to law enforcement officers truthful information relating to the commission or possible commission of any federal offense,

Third: WS provided information to Special Agents of the Federal Bureau of Investigation.

4. The essential elements of Count Two of the superseding information alleging a violation of 18 U.S.C. §371, that is Conspiracy to commit Access Device Fraud (18 U.S.C. §1029(a)(9)) and Unauthorized Access of Protected Computer (18 U.S.C. §1030(a)(5)(A)(ii) and (B)(iv)), are that

First: The defendant and at least one other person made an agreement to commit the crime of Access Device Fraud (18 U.S.C. § 1029(a)(9) as described below, or Unauthorized Access of Protected Computer (18 U.S.C. §1030(a)(5)(A)(ii) and (B)(iv)), as charged in Count Two of the superseding information;

Second: The defendant knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and

Third: One of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in Count Two of the superseding information, in order to accomplish some object or purpose of the conspiracy.

5. The essential elements of the object of the conspiracy alleged in Count Two of the superseding information, that is Access Device Fraud (18 U.S.C.§1029(a)(9)), are that

First: The defendant or another coconspirator knowingly used and controlled hardware and software of a telecommunications instrument, that is the access codes to telecommunications equipment to affect caller identification information;

Second: By such use and control as described above, the defendant knew that caller identification information had been altered and modified; and

Third: By such use and control as described above, the defendant knew that the caller identification information had been altered and modified so that the telecommunication instrument could be used to obtain telecommunications service without authorization.

6. The essential elements of the object of the conspiracy alleged in Count Two of the superseding information, that is Unauthorized Access of Protected Computer (18 U.S.C. §1030(a)(5)(A)(ii)) and (B)(iv), are that

First: The defendant or another coconspirator intentionally accessed a protected computer belonging to a telecommunications service;

Second: The protected computer was a computer used in interstate or foreign commerce or communication;

Third: The defendant or another coconspirator accessed the protected computer without or in excess of authorization; and

Fourth: During the unauthorized access to the protected computer, the defendant or another coconspirator recklessly caused damage and engaged in conduct constituting a threat to public health or safety.

FACTUAL STIPULATIONS

Defendant Matthew Weigman (Weigman) stipulates and agrees to the following facts in support of his plea of guilty:

1. During all times relevant to the offense, Weigman lived in the state of Massachusetts.

2. "Swatting" meant placing a telephone call to a police department from a spoofed telephone number and falsely reporting an emergency situation at the address associated with the spoofed telephone number in order to cause a law enforcement swat team to respond to the hoax call at the address.

3. "Social engineering" meant to impersonate someone, i.e. a telephone system employee or other person, in order to gain the cooperation of an unsuspecting party in order to obtain information or unauthorized access to telephone systems. Weigman, codefendant Carlton Nalley, and others obtained name, address and phone number information for use in swatting from social engineering techniques on telephone company employees and others.

4. To "spoof" meant the act of falsifying Caller I.D. information to conceal the true Caller I.D. of a telephone call.

5. A "spoof card" is a type of commercial account accessible either online or by telephone which provides an access device, i.e. a number or computer code, which enables the caller to elect a number of services including the concealment of the caller's true Caller I.D. by substituting another Caller I.D., changing the caller's voice to another

gender, and/or recording the call on the company's servers.

6. Weigman had been and was being investigated by the Federal Bureau of Investigation (FBI) for Weigman's participation in swatting activities.

7. In order to make the swatting calls, Weigman and others, to include Stuart Rosoff, Jason Trowbridge, Chad Ward, Guadalupe Martinez, and Angela Roberson (defendants named in the Northern District of Texas (NDTX) indictment *United States v. Stuart Rosoff, et al*, 3:07-CR-196-B) (jointly referred to as *Rosoff* defendants), would make unauthorized access to telecommunication company information stored on protected computers in order to obtain name, address and phone number information of their intended targets, and to use software and hardware configured to insert or modify telecommunication access devices and account information for telephone customers and employees, in order to obtain free telephone service or discontinue service for telephone subscribers. Approximately 15-20 participants in the telephone party lines including Weigman, Nalley, and the *Rosoff* defendants, agreed to participate and did participate in targeting, executing and obtaining information to facilitate swatting calls.

8. To begin a swatting call, Weigman and others would fraudulently obtain the personal identifiers, such as passwords and access codes, addresses, and telephone numbers, of certain telecommunication employees. Weigman and others would impersonate the customer of the targeted telephone number, impersonate the telecommunications employee capable of initiating changes to the targeted telephone number, and/or establish fraudulent telephone accounts.

9. Other individuals associated with Weigman pled guilty to swatting related conduct in the *Rosoff* Indictment in the NDTX.

10. Beginning at least in or about June 2003, and continuing through on or about May, 2008, Weigman participated in multiple telephone party line chat groups (party lines) with Nalley, the *Rosoff* defendants, and other coconspirators. Weigman, Nalley, the *Rosoff* defendants, and others agreed among themselves to conduct swatting calls for the purpose of harassing targeted individuals, many of whom were participants in the party lines, and their families.c

11. During the conspiracy, Trowbridge obtained personal identifying information on individuals for use in swatting activities by using a computer and exceeding his authorized access to Accurint databases. Accurint is a commercial database on protected computers used in interstate and foreign commerce containing consumer information from the files of a consumer reporting agencies, banking institutions and credit card companies. Weigman and others also obtained name, address and phone number information for use in swatting by using social engineering techniques on telephone company employees and others. Other coconspirators also obtained information from social engineering and other databases.

12. In or about June 2006, Weigman and others agreed to "swat" Victim#1 of Alvarado, Texas. Victim#1's daughter was a partyline participant who lived in Fort Worth, in the NDTX. Weigman made harassing calls to Victim#1's residence using a spoof card he had obtained from Rosoff that had originated with Ward. Trowbridge

provided name, address and telephone information about Victim#1 to facilitate swatting calls to Victim#1 by exceeding his authorized access to the Accurint database. Martinez used the information provided by Trowbridge to make a swatting call resulting in a police response to Victim#1's residence on June 12, 2006. On June 12, 2006, Martinez placed a spoofed call to the phone number for non-emergency services for the Alvarado Police Department, Alvarado, Texas using a voice over internet protocol phone (VoIP) and a spoof card to conceal his true identity, in order to make it appear to emergency services that the call was actually made from Victim#1's residence. Martinez identified himself as Victim#1 and told the dispatcher that (1) he had shot and killed members of Victim#1 family, (2) he was holding hostages, (3) he was using hallucinogenic drugs, and (4) he was armed with an AK47. Martinez demanded $50,000 and transportation across the U.S. border to Mexico, and threatened to kill the remaining hostages if his demands were not met. In advance of the "swat," Trowbridge also made harassing calls to the residence of Victim#1 on June 4, 2006, using a spoofcard to alter his Caller I.D. information to make it appear as if the call originated from Victim#1's daughter's residence in the NDTX.

13. On or about October 1, 2006, Ward offered money to anyone who would make a swatting call to Victim#1's daughter. Members of the conspiracy provided Martinez with Victim#1's daughter's address which was obtained from the unauthorized monitoring of Victim#1's daughter's calling information on a telephone system server in violation of 18 U.S.C. § 1030(a)(5)(A)(ii). Subsequently, when Martinez made a phone call directed to

the non-emergency services telephone number of the Fort Worth Police Department to make a swatting call targeting Victim#1's daughter, the call transited AT&T telephone company equipment located in the NDTX in the normal course of call routing. On October 1, 2006, Martinez called the 911 non-emergency services telephone number for the City of Fort Worth Police Department, Fort Worth, Texas and identified himself as Victim#1 and stated that he had shot and killed members of Victim#1's family, that he was holding hostages, that he was using hallucinogenic drugs, and that he was armed. Martinez told the police dispatcher that he would kill the remaining hostages if his demands were not met. Martinez placed the call using a voice over internet protocol phone (VoIP) and a spoof card to conceal his true identity, in order to make it appear to emergency services that the call was a true emergency from Victim#1's daughter's address.

14. Continuing through November, 2006, harassing and threatening calls were made by coconspirators to Victim#1's daughter and on or about November 22, 2006, Ward offered another monetary reward for anyone who would "swat" Victim#1. Trowbridge again exceeded his authorized access to the Accurint database to obtain name, address and telephone number information about Victim#1, which he then provided to the conspirators for use in making swatting calls and in making threatening phone calls.

15. Beginning in or about August 2006 and continuing through October 2006, Weigman, in furtherance of the conspiracy, made more than 50 telephone calls to the Verizon Provisioning Center located at Irving, Texas and obtained unauthorized access to the computers located there and used that access to obtain telecommunications services including Caller I.D. blocking and call forwarding. The computers which Weigman accessed were used in interstate and foreign communication. Weigman also used the Verizon computers to initiate new accounts and services for use in concealing Caller I.D. by the coconspirators, and to terminate services to victims. Weigman and Rosoff also made unauthorized access to telecommunications provider computers and obtained account subscriber information which was used to identify personal information for targeting victims. Weigman bragged about these activities on the party line. In 2004, Nalley and Weigman were active on telephone party lines where they and others would associate, plan, and execute their criminal conduct. In 2004, Weigman joined the party line and began providing direction to Nalley and others. The coconspirators regularly used the caller identification of others, especially their victims, without permission in order to conduct their criminal activity. By using the phone number of their victims, they obtained credit cards, information, and valuable telephone service for which the true subscribers were required to pay. Weigman with the assistance of his coconspirators obtained, via fraud, telephone service for himself and others valued in excess of $30,000.

16. The Verizon computer located at the Verizon Provisioning Center in Irving, Texas was located in the NDTX, and was a protected computer used in interstate and foreign communications pursuant to 18 U.S.C. § 1030(e)(2)(B).

17. Weigman, Rosoff, and others provided telephone numbers and pass phrases which were used by coconspirators to obtain unauthorized access to telecommunications service provider computers. Weigman and Rosoff obtained the telecommunications service access devices including telephone numbers, pass phrases, employee identification numbers, and employee account information used by the conspirators by various means including through "social engineering" or pretexting of telephone calls to telecommunications company employees, "war dialing", trafficking in pass phrases and access information with other phone "phreakers," etc. The unauthorized access to telecommunications computers obtained by Weigman and Rosoff provided Ward and others with unauthorized telecommunications services. Weigman and Rosoff also used their unauthorized access to telecommunications computers to terminate services to individuals, and to initiate unauthorized services for themselves and others. In addition, Weigman told Rosoff that he used unauthorized access to telecommunications computers to engage in unauthorized eavesdropping on private telephone conversations.

18. On July 5, 2006, Weigman called Trowbridge using a spoofcard and provided Trowbridge with the "monitor codes" for a party line in Chicago. Trowbridge subsequently used these "monitor codes" to disrupt service to the party line, including forcing members of the partyline from the party line. Trowbridge invited Angela

Roberson to assist him in this activity. Trowbridge was not authorized to have or use the monitor codes, and his use of the codes to disrupt the telecommunications computers which directed the party line was in violation of 18 U.S.C. § 1030(A)(5)(ii).

19. During the course of the conspiracy, Trowbridge purchased at least one spoofcard which was used to make harassment calls in furtherance of the conspiracy. Rosoff and Weigman received commercial spoof cards and other compensation from codefendant Ward in payment for services and in support of their activities in the conspiracy.

20. During the course of the conspiracy, beginning on or about April 12, 2006, Rosoff transmitted threats and extortionate demands to NJ of Cheboygan, Michigan, in interstate communications. Rosoff threatened NJ that unless she provided him with phone sex, a thing of value, he would turn off her phone service which would prevent her from doing business and cause her monetary loss. She did not comply, and Rosoff used social engineering to terminate her phone service in violation of 18 U.S.C. § 1030(a)(5)(A)(ii). He then contacted the Cheboygan County Department of Human Services and made false reports of NJ's children being abused by her boyfriend for the purpose of causing a police response at her residence. When NJ continued to refuse to provide Rosoff with phone sex, Rosoff enlisted Weigman, Dialtech, and Trowbridge to assist him. On April 22, 2006, Rosoff in a party line with Weigman present, asked Trowbridge to exceed his authorized access to the Accurint database to obtain the name, address and telephone number information on NJ and her boyfriend in violation of 18 U.S.C. § 1030(a)(2)(A) for use in harassing her. Trowbridge complied and provided Rosoff with the information.

Trowbridge and Rosoff then discussed the best way to cause NJ bo be arrested.

21. During the course of the conspiracy, Weigman requested, participated in, or monitored harassing interstate communications to employers, landlords, families , and friends of multiple party line participants with the intent to damage the reputation of those participants, cause them to lose their jobs, or cause them to be evicted. If the threats against the participants were not effective in stopping them from using the party line, the party line participants and, on occasion, their friends and family members were "swatted." Party line participants who were victimized by the members of the conspiracy including Trowbridge, Rosoff, Ward, Roberson, Martinez, Weigman, and others known and unknown to the Grand Jury in this manner include DS of Ormond Beach, Florida; JC of Binghamton, New York; DW of McLean, New York; DH of Nevada, a family in Virginia, Victim#1 in Colorado, Weigman's landlord, hotels in Washington state, and hundreds of others. To facilitate these swats, Trowbridge and others supplied name, address and telephone number information on party line participants by exceeding his authorized access to the Accurint database in violation of 18 U.S.C. §1030(a)(2), while Rosoff, Weigman and others obtained unauthorized access to telephone company computers in order to turn phone service off to prevent police or other emergency responders from calling the victim to determine that it was a hoax emergency.

22. Weigman and other coconspirators also used their ability to manipulate the phone system to listen to phone conversations without permission for both pleasure and financial gain. Weigman was able to obtain unauthorized access to a phone line belonging to Sprint which was used by Sprint supervisors to monitor their customer department. This line was used to monitor Sprint employees as they had conversations with customers and is one of the lines referred to when a customer hears "this line may be monitored for your convenience." Weigman would listen in on this line and wait for a customer to provide a Sprint employee with a credit card number or other valuable information and would then memorize this number and have Nalley or others write it down for him. he then used these numbers to order goods and services for himself and his coconspirators which would be billed to the victim of his unauthorized wire interception. From 2004 through 2008 Nalley assisted Weigman and other coconspirators in obtaining credit cards belonging to others, including United States Government Credit Cards which were for use by the United States Military. Nalley stored and maintained these credit cards for Weigman and other coconspirators and used them to buy items that they wanted such as computers and other electronic equipment valued in excess of $5,000. Nalley stored the credit cards for Weigman in various e-mail accounts he set up for those purposes and provided the credit card numbers to Weigman when Weigman wanted them. Both knew that the credit card numbers were stolen, and both traded those credit cards with other individuals for services or money. Nalley assisted Weigman in obtaining credit card numbers by listening in on customer service calls to various companies.

23. Weigman was aware as of December 2006 that he was a target of an federal investigation, in that the FBI executed a search warrant at Weigman's house. Weigman knew that the FBI was obtaining information from various local law enforcement officers, some of whom had visited Weigman previously, and from investigators at the telecommunications companies, including WS from Verizon.

24. In 2007, law enforcement arrested Martinez, Rosoff, Ward, Trowbridge, and Roberson as a result of the *Rosoff* indictment. Weigman was aware of these arrests and subsequent plea agreements reached with his coconspirators. The *Rosoff* defendants pled guilty to conspiracy charges, and were sentenced for their roles in an ongoing conspiracy to threaten, extort, commit wire fraud, and commit computer fraud. Weigman was also aware that WS of Verizon was testifying for the government and providing the government with records and other documents. From at least 2006 and continuing through and including May 2008, Weigman knew that WS, while acting in his capacity as a Verizon Fraud investigator, provided information and testimony to law enforcement officers, including FBI Special Agents, relating to the commission of federal offenses involving Verizon equipment, by Weigman, Nalley, the *Rosoff* defendants, and other individuals.

25. WS resided and worked in New Hampshire. WS was a fraud investigator for Verizon, a telecommunications provider.

26. WS provided information to the FBI in the *Rosoff* swatting investigation. WS also provided information to the FBI regarding Weigman's conduct.

27. WS was investigating Weigman, and during the spring of 2008 caused a telephone number fraudulently obtained by Weigman to be disconnected.

28. WS's interference with and reporting to FBI of Weigman's criminal activities angered and frustrated Weigman.

29. Weigman wanted to retaliate against WS for investigating him, interfering with his's criminal activities, and reporting his criminal activities to law enforcement.

30. From in or about April 2008 through in or about May 2008,Weigman, Nalley, Benton, and others did knowingly combine, conspire, confederate and agree to retaliate against WS by unlawfully taking an action harmful to WS, who they knew to be a witness in an official proceeding, the *Rosoff* case, with the intent to retaliate against WS. Weigman, Nalley, and others attempted to interfere with the lawful employment or livelihood of WS, for providing to a federal law enforcement officer truthful information relating to the commission of federal offenses by Weigman, Nalley, and others, in that Weigman and Nalley made telephone calls to WS's employer, Verizon, and provided false and misleading information, in an attempt to cause WS's employment to be terminated or for him to be reprimanded.

31. Further, leading up to the telephone calls to Verizon, Weigman manufactured evidence such as spoofed telephone calls to Nalley's phone in an effort to provide false evidence of WS's misconduct in furtherance of the conspiracy.

32. From in or about April 2008 through on or about May 18, 2008, Weigman and Benton, did knowingly combine, conspire, confederate and agree with each other to retaliate against WS by driving to the residence of WS in an effort to intimidate and frighten WS. They agreed that they should travel to WS's residence in another state in order to cause him to cease his activities. They were aware that WS's cooperation assisted law enforcement in the investigation and prosecution of other party-line participants involved in swatting activities with Weigman.

33. Weigman advised Benton that he (Weigman) and others had already manufactured false evidence and "filed" a false claim with Verizon in an effort to cause WS to be fired. Weigman told Benton that he had already placed numerous intimidating and harassing calls to WS and that he was monitoring WS's phones. Weigman and Benton discussed what they would say if stopped by law enforcement, including providing false names, and agreed on how best to cause WS to allow them to continue their criminal conduct unimpeded. On May 18, 2008, Weigman, his brother, and Benton traveled to WS's residence in Benton's car. Upon their arrival at the residence, Weigman asked Benton to write down tag numbers or descriptions of any vehicles at the residence. WS was not home initially, but arrived soon after Weigman's and Benton's initial appearance. Weigman and Benton confronted WS on May 18, 2008. Weigman and Benton intended by their appearance with Weigman's brother, to harass and intimidate WS and to cause WS to stop investigating and reporting to law enforcement the criminal conduct

of Weigman and others.

34. In April and May of 2008, Weigman gained unauthorized access to the phone system at a book store which he then used to place harassing calls to WS. After Verizon identified a phone line that Weigman had obtained by fraud in April 2008, and turned the phone line off, Weigman used the identities and authorization codes of Verizon employees to have the phone reactivated. Weigman also used his ability to gain unauthorized access to the phone system to conduct unauthorized electronic monitoring of Verizon employees' phones in order to harass the employee and obtain information about the status of the investigation against Weigman. Weigman directed others to obtain the personal identifying information of verizon employees in order to harass them and used his own skill at social engineering to obtain information his coconspirators could not.

I have read (or had read to me) this Factual Resume and have carefully reviewed every part of it with my attorney. I fully understand it and voluntarily agree that the facts recited herein are true and correct.

MATTHEW DOUGLAS WEIGMAN
Defendant

Jan. 23, 2009
Date

I am the defendant's counsel. I have carefully reviewed every part of this Factual Resume with the defendant. To my knowledge and belief, my client's decision to sign the Factual Resume is an informed and voluntary one, and that according to my client the facts recited herein are true and correct.

CARLO D'ANGELO
Attorney for Defendant

Jan. 23, 2009
Date